Приложение №2
„ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ“

I. Въведение

С настоящите изисквания се определя минималното ниво на технически и организационни мерки при обработване на лични данни и допустимия вид защита, съгласно чл. 28 ал. 3 от ОРЗД.

Приложение №…… към „Споразумението за обработка на лични данни“, има за цел да осигури адекватно ниво на защита на личните данни в поддържаните регистри с лични данни от случайно или неправомерно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други неправомерни форми на обработване.

Обработващият лични данни предприема необходимите технически и организационни мерки за защита на личните данни, за да гарантира адекватно ниво на защита, което отговаря на обработваните лични данни и въздействието при нарушаване на защитата им. Мерките имат за цел да гарантират поверителност, цялостност и наличност на личните данни.

II. Видове защита

1. Задължения на персонала на Обработващия лични данни.

Обработващият данните следва да прилага мерки спрямо своите работници/служители, които обработват лични данни, предоставени от Администратора. Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа "Необходимост да знае".

Конкретни мерки към работници/служители, обработващи данните:

- познаване на нормативната уредба в областта на защитата на личните данни;
- познаване на политиката и ръководствата за защита на личните данни;
- задължение за запазване на конфиденциалността между персонала (например идентификатори, пароли за достъп и т.н.) във връзка с обработване на личните данни
- съгласие за поемане на задължение за неразпространение на личните данни;

- провеждане на обучения;

2. Физическа защита

Физическата защита на личните данни представлява система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и обекти, в които се обработват лични данни, а именно:

- Наличие на зони с контролиран достъп - охрана и/или система за сигурност;
- Използване на технически средства за физическа защита – ключалки, шкафове, метални каси и др.;
- Наличие на правила за размножаване, разпространение и процедури за унищожаване;
- Наличие на обособени помещения, в които се разполагат елементите на комуникационно-информационните системи за обработване на лични данни;
- Наличие на пожароизвестителни и пожарогасителни системи;
- Наличие на вътрешни правила за действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.);
- Наличие на контролиран и персонализиран достъп до регистри с лични данни;
- Спазване на определените от Администратора срокове за съхранение на личните данни;
- Наличие на процедури за проверка и контрол на обработването.

3. Информационна сигурност

Всички информационни системи трябва да отговарят на изискванията и добрите практики за мрежова и информационна сигурност. Необходимо е да бъде подсигурена защитата им срещу неправомерен или случаен достъп, неконтролирано използване, нерегламентиран достъп на трети лица, промяна или унищожаване на автентичността, целостта и конфиденциалността на съхраняваните или предаваните данни.

Обработващият лични данни е длъжен да:

- Защитити информационните системи и комуникационни мрежи, чрез които обработва данните, използвайки различни технологии като защитни стени и криптография.
- организира комплексни проверки за оценяване степента на постигнатата мрежова и информационна сигурност в използваните от него информационни системи;

- вземе мерки за предотвратяване на неправомерен достъп от трети лица до ресурсите на неговите информационни системи – идентификация, автентификация, контроли на сесията;
- осигури условия, при които неоторизирани лица не могат да получат физически достъп до работните станции, сървърите и/или масивите за данни;
- следи за неправомерно инсталиран софтуер на работните станции или сървъри и взема мерки за неговото отстраняване;
- осигури защита срещу нежелан софтуер в информационните системи;
- да разполага със системи за разпределение и управление на криптографските ключове при използване на криптография за защита на данните;
- осигури мониторинг на събитията и инцидентите, настъпили в използваните от него информационни системи, като създава указания за извършването му в утвърдените от него вътрешни правила;
- осигури нива на достъп на различните групи служители до ресурсите в информационните системи - определяне на роли и отговорности;
- осигури копия/резервни копия за възстановяване на информационните системи;
- имплементирана процедура за унищожаване/заличаване/изтриване на носители на данни.